Hillstone
山 石 网 科

山石网科iWAF（极速·智御）系列

W3060-GC-B

在科技飞速发展的今天，网站和 Web 应用系统正面临着日益严峻的安全挑战，威胁数量不断增加，资产规模也呈爆炸式增长。这不仅要求精准的资产识别与检测能力，还带来了网络流量的激增，对传统 WAF（Web 应用防火墙）的性能提出了前所未有的挑战。在此背景下，山石网科 Web 应用防火墙（WAF）进行了全面升级，推出了**全新的 iWAF（极速·智御）系列**。其中的“i”蕴含着两层深刻含义：

inline 极速架构：采用了先进的 FPGA 及 ASIC 硬件加速方案。这种创新的串联部署模式，能够实现毫秒级响应和百 G 吞吐量，确保在提供超高性能的同时，构建起高可靠性的安全防护屏障。

*ASIC 芯片卸载 算力全面释放：*通过 ASIC 芯片卸载非 HTTP 流量，实现线速转发，大幅降低整机 CPU 占用，为资产自发现和安全防护释放充足算力，保证资产识别的覆盖度与精度。

*多级逃生机制 业务稳定性拉满：*软件 Bypass 触发时，由 ASIC 芯片接管流量转发，几乎不占用 CPU 资源，避免业务中断。

硬件 Bypass 支持 25G/40G/100G 等高规格光口硬件 Bypass 方案，实现从软件到硬件的多级业务逃生，保障极端场景下的业务连续性。

intelligent 智御体系：搭载了站点自发现、默认防护以及 GenAI 智能分析引擎，使得 iWAF 无需复杂配置，即可智能精准地识别各类威胁，实现从被动防御到主动预判的转变，解决资产暴露的检测难题。

产品价值

保护网站和关键业务系统

网站是政府机关和企事业单位对外展示形象的窗口，对于一些行业来说，网站也是重要的业务支撑系统。山石网科 WAF 能够对各种网络层和应用层攻击进行检测和防御，比如包括注入攻击、跨站脚本(XSS)攻击、漏洞攻击在内的 OWASP (Open Web Application Security Project，开放 Web 应用安全项目)十大安全风险，网络层及应用层 DDoS 攻击，暴力破解攻击等，确保网站和关键业务系统的稳定运行。

满足等级保护合规要求

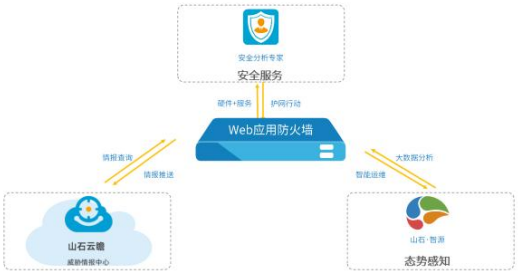
根据网络安全法和《网络安全等级保护条例》的要求，网络运营者应当"…保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改"。相对于内网，暴露在互

联网中的网站更容易遭受黑客的攻击和篡改，在这种情况下，网站运营者既是受害者，又是责任的承担者。山石网科 WAF 帮助网站运营者防患于未然，满足合规要求。

产品亮点

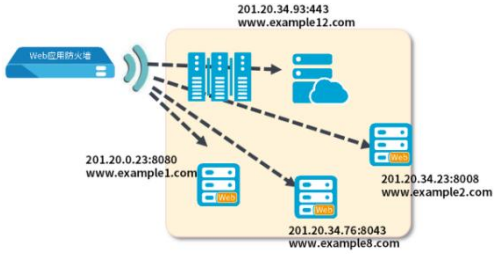
可持续安全运营

山石网科WAF支持威胁情报中心情报推送&查询;检测数据可以上送态势感知平台进行全网智能运维分析;同时还可以结合山石网科安全服务团队，以硬件+服务的形式提供服务，助力客户实现可持续安全运营。



智能的web资产自发现

随着应用的扩展，需要保护的网站可能达上百个之多，且分散于不同的业务部门。山石网科WAF支持智能Web资产自发现，可以自动侦测系统中的 Web 网站，并一键添加为保护对象，不漏掉一个保护。



主动防御默认站点

随着业务的拓展，Web 应用防火墙部署形态也逐渐增加，但无论使用哪种部署模式，均需要手动配置站点，才可以对网站进行防护。但随着需防护的网站数量的增加，配置站点需要消耗大量的时间与精力，无法做到即插即用快速上线防护。山石网科 Web 应用防火墙支持默认站点实现对各网站的快速防护。没有复杂的策略配置及繁琐的站点配置，无服务 IP、端口及域名数量的限制，一键开启默认站点防护，实现快速上线，快速防护，快速阻断攻击。

静态及动态网页防篡改

网站篡改的技术门槛低，传播速度快，社会影响大，是黑客经常采用的攻击手段。山石网科WAF通过缓存技术对静态网站提供防篡改功能，同时对基于SQL注入的篡改行为进行阻断。配合山石网科网页防篡改系统，可以实现对动态网页的篡改防护，确保从源头解决篡改难题。

关键资产重保模式，一键提升防护等级

山石网科 Web 应用防火墙针对重保场景，定制有针对性的重保防护策略模板，针对重保期间常见的安全威胁进行重点防护，提供一键配置向导，规则库更新频率调整为小时检测更新，更快响应 0day 规则更新。满足了重保期间业务高效、安全、稳定运营。

集成专业防火墙能力，安全能力全面

山石网科 WEB 防火墙集成专业的防火墙策略控制功能，WAF 的策略可通过源 IP 地址、目的 IP 地址、源端口、目的端口以及传输层协议这五个关键元素，为网络流量提供了精确而灵活的控制手段。五元组控制不仅能够在复杂的网络环境中快速准确地识别并拦截潜在的安全威胁，还能根据业务需求自定义安全规则，确保只有符合预设规则的流量能够通过网络。此外，山石 WAF 具备策略分析、优化能力。

专业一虚多，一台设备当多台用

山石网科 WAF 的 VSYS 功能是一项强大的创新技术，它允许用户在一台物理 WAF 设备上创建多个逻辑上独立的虚拟 WAF 系统（VSYS）。通过 VSYS 功能，管理员可以根据业务需求，轻松创建、配置和管理多个独立的 WAF 系统，每个 VSYS 都拥有自己独立的安全策略和站点配置等。

API 防护保障，防范数据泄露风险

API 防护策略的功能是山石网科 WEB 应用防护墙网站安全管理的核心组成部分，其重要性不容忽视。

通过这一功能，用户可以定制一套全面且细致的防护措施，确保 API 流量的安全性和合规性。具体来说，API 防护策略允许用户根据业务需求和安全要求，设置各种检测规则，如 URL、请求头、参数和请求体的校验，以识别并拦截潜在的恶意请求。这些规则可以基于 OpenAPI 规范文档进行配置，也可以由管理员根据具体情况自定义，从而实现对 API 流量的精准控制。

双引擎检测-语义分析+规则匹配

通过业内创新的语义分析+规则匹配双引擎检测技术，结合词法/语法分析，基于理解语言规范基础上，结合上下文进行关联分析，支持多层递归解码还原威胁，检测率大幅上升。

大屏可视

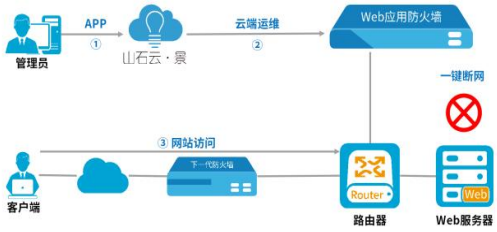
山石网科WAF支持大屏可视，支持中国地图与世界地图切换，更动态、直观的展示攻击趋势；支持展示设备热点威胁事件，最新威胁事件；支持展示站点威胁的等级分布，风险站点，站点总数，站点性能。

实时检测网站健康，异常一键关停

敏感网站一旦被黑客攻破或篡改，就需要快速关停避免损失扩大。通过山石网科云景APP，联动山石网科WAF防篡改功能，可以实时监测网站是否被篡改，自动实现3分钟快速关停被篡改网站，避免损失进一步扩大。

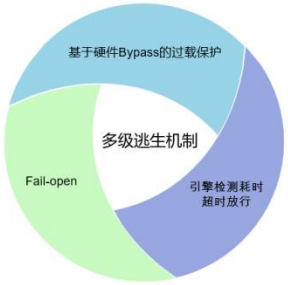
敏感信息防泄露

敏感信息加星，不影响正常业务：个人信息防泄漏：手机，邮箱，身份证，银行卡号等；敏感词防泄漏：敏感政治倾向、暴力倾向、不健康色彩。



多级逃生机制

多级逃生机制，逃生方式包括引擎检测耗时超时放行；Fail-open；基于硬件Bypass的过载保护。层次化的多级逃生机制可提高业务的高可用性，保障业务平稳运行。



智能日志分析+多级日志聚合

智能日志分析（误报分析+威胁分析） + 多级日志聚合，精简海量日志，降低运维成本。

功能规格

Web应用防护

- 系统具备 HTTP 协议异常防御能力
- 支持 SSL 透明代理，可以对 HTTPS 网站进行保护
- HTTPS 站点支持证书链检测
- 支持通过 X-header 传递客户端证书信息或完整客户端证书的传递，实现服务端针对客户端的证书校验
- 针对 HTTP 快速 Flood 和慢速 Flood 攻击进行防护
- HTTP Flooding，暴力破解攻击支持基于用户 IP 统计以及验证码，速率限制等多种防护方式
- 系统具备注入攻击防御能力，可以对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、远程文件包含、本地包含、代码注入、邮件注入、XML 注入以及其它注入进行防御
- 系统具备跨站攻击防御能力，可以对 XSS 和 CSRF 攻击进行防御
- 系统具备对 SQL 注入和 XSS 攻击的智能语义检测能力
- 支持配置不同的 XSS /SQL 注入语义检测规则敏感度，以防护不同级别的威胁，提高检测的精准度
- 系统具备信息泄露防御能力，可以防止服务器错误、数据库错误、Web 目录内容、程序代码、关键字（支持中文）等信息的泄露
- 具备个人敏感信息防泄漏功能，可以检测到个人身份信息（包括中国大陆身份证号、港澳台身份证号、美国社会安全号）、银行卡号、信用卡号、邮件账号的信息泄露，支持对敏感信息的脱敏操作（替换为指定字符）
- 系统具备保护 Cookie 安全能力，可以防止 Cookie 被恶意篡改、Cookie 被恶意劫持，支持 Cookie 签名和 Cookie 加密功能
- 系统具备探测访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御
- 支持基于客户端 IP 对 HTTP 访问进行细粒度控制，可以匹配 HTTP 操作方法、HTTP 头名称、HTTP 内容类型、HTTP 协议版本、URI 路径等
- 系统具备特殊漏洞攻击防御能力，针对 Web 服务器、Web 框架、Web 应用程序的漏洞及其它漏洞攻击进行防御
- 系统具备防御资源非法访问能力，可以对非法上传、非法下载和盗链攻击进行防御，支持根据文件大小、MIME 文件类型、扩展名进行非法下载控制，非法上传支持依据文件内容和文件扩展名检测文件类型
- 系统具备恶意软件防御能力，针对 WebShell、木马攻击等进行防御
- 系统具备防暴力破解攻击能力
- 部署在负载均衡设备或代理服务器之后时，可以解析源 IP 地址，支持 X-Forward-For 和 TCP Option 获取客户端真实源 IP，对客户端的真实 IP 进行阻断
- 支持用户自定义规则；支持全局自定义规则开关与时间表
- 提供预定义防护策略模板，支持自定义防护策略，自定义规则支持配置防护子类型
- 特征库支持网络实时更新
- 支持 API 的安全检测和防护功能，可基于 OpenAPI 规范文档，实现合规性检测
- 支持配置站点状态为网站维护状态
- 支持配置站点状态为转发状态
- 支持批量修改站点配置(站点状态、安全策略仅告警、Web 访问日志状态、站点安全策略、SSL/TLS 证书链、报表)
- 支持重保模式，重保模式推荐配置，重保模式配置还原；新增加重保策略，重保策略模板；

网页篡改检测

- 支持学习模式和保护模式两种运行模式
- 支持防护内容的相似度比较
- 支持自定义防护的静态网页类型，支持对例外 URL 不做防篡改保护，支持时间表设置防护时间段
- 内置同步引擎同步服务器内容并建立基线
- 支持篡改监控和正常修改监控
- 支持篡改内容取证
- 发现篡改行为时，支持一键断网阻止对网站的访问

Web漏洞扫描及虚拟补丁

- 产品支持 Web 应用漏扫
- 支持扫描各种类型的 Web 漏洞包括：SQL 注入漏洞、XSS 攻击漏洞、Web 服务漏洞、信息泄露漏洞、异常访问漏洞
- 支持普通扫描和侵入式扫描
- 支持对需要认证的 Web 页面进行扫描

- 支持对目录深度、链接总数、文件数进行限制
- 支持手动扫描和定期扫描，可以定期自动扫描
- 扫描报告支持导出，支持 PDF、XML 文件报告
- 虚拟补丁支持 appscan 报告

网络安全防护

- 支持根据漏洞扫描结果，或者导入的报告生成虚拟补丁，对网站的漏洞进行快速保护
- 支持抗拒绝服务攻击，包括：Ping of Death、Teardrop 攻击、IP 分片攻击、Smurf 及 Fraggle 攻击、Land 攻击、ICMP 大包攻击等
- 支持对 DNS 查询洪泛攻击进行防护，可以根据源和目的设置警戒值
- 针对 TCP 协议异常的防护
- 针对 IP 地址扫描/欺骗、端口扫描进行防护
- Flood 防护包括 ICMP Flood、UDP Flood、SYN Flood 等
- 支持基于源/目的 IP、源/目的安全域、服务、时间表等配置策略进行包过滤，支持策略组，支持策略优化（策略命中分析、冗余检测、策略助手）
- 支持 IP 信誉库，阻断恶意 IP
- 联动山石云·景 APP，实现一键断网
- 支持 Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Referer、Cookie 等 HTTP 头部的策略控制
- 在串联、牵引、单臂和反向代理模式支持 HTTP2
- 6to4 场景支持通过 X-header 中的 ipv6 地址进行安全防护
- 在旁路监听模式下支持 HTTPS 解析，支持 IPv6 流量的检测
- 访问控制策略支持时间表

IPv6协议

- 支持 IPv4、IPv6 双栈部署，可同时添加 IPv4 和 IPv6 地址为保护站点

自学习策略

- 支持对 IPv4/IPv6 访问流量的检测和保护
- 支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略
- 学习的内容包括：动态 URL 地址、URL 参数、HTTP 访问方法、Cookie 等信息
- 支持学习模式和保护模式，学习完成后可以自动切换到保护模式
- 支持 URL 访问量统计以及 URL 最短/最长/平均访问耗时统计
- 支持对特定 URL 例外，不进行学习

防御动作

- 支持对触发规则行为仅告警
- 支持针对触发安全规则的行为进行阻断并发出告警页面
- 支持用户对阻断告警页面进行自定义
- 支持告警页面重定向至其它 URL
- 支持以安全日志为入口添加白名单（例外规则），支持基于 URL、源 IP、HTTP 头部、请求行参数和请求体的例外规则，支持基于全局和基于站点的规则例外
- 支持将攻击者加入黑名单，对后续的访问进行阻断
- 支持 IP,URL 黑名单及 IP,URL/域名白名单；支持基于时间表的动态 IP 白名单
- 支持与防火墙联动，下发黑名单
- 根据 GeoIP 进行访问控制，支持限制国外地区的访问
- 联动威胁情报平台，对发现的威胁事件，查询相关 IP、文件的威胁情报详情
- 支持从威胁情报平台获取热点威胁情报信息

部署模式

- 支持透明串接部署，无需变更网络配置
- 支持镜像监听部署，无需变更网络配置；支持攻击阻断
- 支持反向代理部署
- 支持单臂部署模式
- 支持牵引部署模式，包括 PBR 回注和跨接回注；支持默认站点
- 支持串联监听部署，无需变更网络配置，支持 MPLS 流量检测
- 支持站点自发现，能够发现网络中的 Web 网站，并一键添加为保护站点；支持基于域名过滤进行站点自发现
- 支持默认站点，提高上线的效率
- 支持单臂模式和反向代理模式下，站点配置非接口 IP，并支持 ARP 应答
- 支持图形化部署向导
- WAF 多站点支持路由隔离

虚拟化部署

- 支持虚拟化，可以在 VMware、KVM、Openstack、Xen 平台上部署
- 支持内置 Agent, 如 VMware Tools 和 Cloud-init

- 支持阿里云，华为云，天翼云，腾讯云，AWS，移动云，百度智能云，EasyStack，华云，宝之云
- 支持在国产 ARM 平台（飞腾、鲲鹏）部署
- 公有云环境中支持 HA 部署（阿里云、AWS）
- 支持通过授权管理系统（LMS）进行授权管理
- 支持 Restful API，可以通过第三方云管理平台进行安全编排
- 支持网卡热插拔、SR-IOV 和弹性扩容，为用户提供可扩展的安全防护能力
- 支持 RESTful API

虚拟系统

- 支持 VSYS

高可用性

- 支持 HA-AP 双机热备功能
- 支持 HA-AA 双主 Peer Mode 模式
- 通过内置或外置的组件，支持断电 Bypass 功能
- 所有标配业务电口都支持硬件 Bypass 功能
- 扩展接口支持内置硬件 Bypass
- 支持软件 Bypass (透明和代理模式下),在 CPU、并发连接数超过阈值时，可优先确保业务连通性
- 支持多级逃生机制
- 支持引擎检测耗时超时放行逃生方式
- 在串联和串联监听模式下, 支持基于硬件 Bypass 的过载保护逃生方式
- 在串联、反向代理、单臂、牵引模式下，支持开启 Fail-open 逃生方式

应用加速及服务器负载均衡

- 支持 Web Cache、页面压缩和 TCP 连接复用，支持 SSL 卸载/SSL 代理，降低 Web 服务器压力
- 支持 SSL 硬件加速
- 支持服务器负载均衡（反向代理和单臂模式下），支持加权轮询、最少连接以及 IP Hash 算法
- 服务器负载均衡支持 IPv6,支持网站 IPv6 改造
- 支持对服务器的健康检查，可以自定义健康检查所使用的 URL 对象
- 支持 X-Header 用作负载均衡 IP
- 支持对 HTTP GET、HEAD、POST 和 PUT 请求的响应内容进行静态资源缓存，减少客户端与服务器的交互次数，加快站点的处理速度

网络及接口配置

- 支持静态路由
- 支持集聚接口
- 支持 Vlan 子接口
- 支持多 vSwitch、virtual-wrie
- 支持 LLDP 协议

设备管理

- 支持 HTTP、HTTPS、SSH、Console 等多种管理方式，支持配置可信管理主机
- 支持多级管理权限设置功能，预定义系统管理员、操作员、审计员等管理角色
- 管理员认证支持：本地认证、Radius、TACAS-C+认证
- 设备运行状态显示，包括硬盘、内存和 CPU、温度利用率的概览显示和详细信息显示
- 支持通过山石网科 HSM 进行集中管理,可以通过山石网科 HSM 进行多台 WAF 设备的集中升级；支持规则库、产品版本信息获取、证书链文件获取、站点性能监控数据上报
- 支持山石云景，用户可以方便的通过手机客户端了解 WAF 的运行状态
- WEB 界面支持 CLI 管理通道
- 支持 CPU 利用率、内存利用率、接口带宽的系统告警规则
- 系统支持 hping/tcpdump/curl/dpdump 运维工具

日志、报表和告警

- 提供丰富的日志信息，包括设备管理日志、网络安全日志、Web 安全日志、防篡改日志、访问控制日志、自学习模型违背日志、Web 访问日志等
- 支持记录攻击事件的 HTTP 所有请求信息， 含请求的 URL、UserAgent、POST 内容， Cookie 等
- 支持记录服务器响应内容信息
- 支持通过电子邮件、SNMP、SYSLOG、短信等多种响应方式进行告警
- 支持多维度日志聚合，可以根据防护规则、客户端 IP 对威胁日志进行聚合显示
- 支持智能日志分析，包括威胁分析和误报分析，可以根据分析结果，对安全策略进行一键优化，提升防护效果
- 支持攻击回放，可帮助管理员快速分析、定位网络中的威胁与攻击。
- 支持误报反馈，将管理员怀疑为误报的日志进行上报
- 支持 Web 安全日志删除功能
- 支持 Web 安全日志导出攻击内容

- 支持日志转存到 FTP 功能
- 支持用户自定义报表
- 支持 PDF、DOC、HTML 格式的报表输出
- 支持周期性报表输出
- 邮件服务器支持 START TLS 和 SSL 加密传输
- 支持用户会话跟踪策略，日志中增加用户名，会话标识符和会话标识值
- WAF 页面支持攻击源显示国家，地区
- 支持报表，提供安全风险概览、站点风险详情、攻击类型详情、站点访问量、网络层攻击汇总、系统运行状况等多维度报表模板
- 支持通过 FTP 及邮件发送报表
- Web 安全日志中支持记录响应报文信息
- Web 安全日志、API 防护日志及自学习模型违背日志中支持显示响应体内容，为用户分析攻击行为提供更多的判断依据
- Web 安全日志记录非 Web 攻击流量，Web 安全日志防护动作颜色标识；Web 安全日志显示优化，客户端 IP 一键“添加过滤条件”
- 支持 PCI-DSS 报表，可根据 PCI-DSS 规范，评估保护站点的合规性
- 支持弱口令检测，包括密码字段、用户名字段及密码复杂度检测配置，支持与用户会话跟踪策略联动，提供账号安全概览
- 支持对 HTTP 协议异常、信息泄露、跨站攻击、探测访问及用户自定义等防护规则产生的 Web 安全日志进行归并，可有效减少日志数量、降低日志误报率
- 支持对站点的 Web 访问日志进行 IP/URL 筛选记录，减少冗余日志

升级支持

- 特征库可以通过人工或者自动方式进行 WAF 设备的升级，升级过程中不需重启设备，并能保持原有会话连接不中断

大屏可视

- 支持中国地图与世界地图切换，更动态、直观的展示攻击趋势
- 支持展示设备感知到的所有威胁
- 支持展示设备热点威胁事件，最新威胁事件
- 支持展示站点威胁的等级分布、站点总数，风险站点
- 支持站点性能展示

虚拟系统

- 允许用户在一台物理 WAF 设备上创建多个逻辑上独立的虚拟 WAF 系统（VSYS）

配置管理

- HTTPS 证书管理，支持证书导出、证书详情查看、有效性检查
- 支持导出打包配置支持导出自定义错误页面、永久阻断黑名单、默认站点配置

硬件规格

型号	W3060-GC-B
产品图片	
管理接口	1个MGT口、1个HA口、1个RJ45串口、2个USB口
HTTP吞吐（网络层）	25Gbps
HTTP吞吐（应用层）	2.5Gbps
固定业务接口	8 × 10GE/GE光 8 × GE电
扩展模块槽位	2个
扩展模块选项	8×GE RJ45，4-bypass 8×GE SFP，支持光转电 1×100GE，QSFP28，支持降速40G，支持1分4*25GE 2对多模Bypass光口 2对单模Bypass光口
硬盘槽位	1
硬盘规格	可选如下规格 SSD：512GB/1TB/2TB/4TB
产品形态	1U
电源规格	交流热插拔双电源
外形尺寸（深*宽*高）	558mm*482mm*44mm
设备重量	净重8.95KG，毛重11.85KG
额定功率	550W
工作环境温度	0-40 ° C
环境相对湿度	10%~95%（不结露）